A REPORT
TO THE
MONTANA
LEGISLATURE

INFORMATION SYSTEMS AUDIT

Statewide Accounting, Budgeting, and Human Resource System

Department of Administration

JANUARY 2008

LEGISLATIVE AUDIT
DIVISION

08DP-03

Fraud Hotline
Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at:

(Statewide)
1-800-222-4446
(in Helena)
444-4446

Information System Audits

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705
(406) 444-3122
Reports can be found in electronic format at:
http://leg.mt.gov/audit.htm

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
Tori Hunthausen,
Chief Deputy Legislative Auditor

Deputy Legislative Auditors:
James Gillett
Angie Grove

January 2008

The Legislative Audit Committee
of the Montana State Legislature:

We conducted our annual Information Systems audit of the Statewide Accounting, Budgeting, and Human Resource System (SABHRS) maintained and operated by SABHRS Services Bureau (SSB) of the Department of Administration (DOA) to assist in the administration financial and human resource records within the state government.

This report contains two recommendations for improving controls over SABHRS access.

We wish to express our appreciation to the Department of Administration staff for their cooperation and assistance.

Respectfully submitted,

/s/ Scott A. Seacat

Scott A. Seacat
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Appointed and Administrative Officials

Department of Administration	Janet R. Kelly, Director
	Paul Christofferson, AFSD Administrator
	Nyla Johnson, SABHRS Services Bureau Chief
	Ed Glenn, Finance Co-Manager
	Martha Watson, Human Resource Manager
	Jim Sheehy, IT Manager

Executive Summary

The Statewide Accounting, Budgeting and Human Resource System (SABHRS) is an enterprise computer application implemented by the State of Montana to assist state agencies and the Montana University System to record the disposition, use , and receipt of public money and property in accordance with state law (section 17-1-102, MCA). SABHRS also assists in the administration of human resource (HR) information, including the generation of a bi-weekly payroll. SABHRS Services Bureau (SSB) at the Department of Administration (DOA) is responsible for the general maintenance, operation, and security of SABHRS.

On an annual basis an Information Systems (IS) audit is conducted over controls residing within the SABHRS application. Audit work focused on ensuring key system controls are working as intended to maintain the integrity of business processes. IS auditors also addressed general security controls that are in place to ensure the security of business processes. This report focuses on general controls; specifically, identifying areas where DOA can improve controls over user access to the SABHRS application.

This report contains two recommendations for development and implementation of review procedures to ensure conflicting access roles are segregated and SSB programmers do not have access to modify programming code and database tables in the production environment.

Chapter I – Introduction and Background

Introduction and Background

The Statewide Accounting, Budgeting and Human Resource System (SABHRS) is an enterprise computer application implemented by the State of Montana to assist state agencies and the Montana University System to record the disposition, use, and receipt of public money and property in accordance with state law (section 17-1-102, MCA). SABHRS also assists in the administration of human resource information, including the generation of a bi-weekly payroll. SABHRS Services Bureau (SSB) at the Department of Administration (DOA) is responsible for general maintenance, operation, and security of SABHRS.

On an annual basis an information systems audit is conducted over controls residing within the SABHRS application. Included in this audit is a review of modifications made to SABHRS to provide a more customized application for state agency users. Based on our work, we provided an internal distribution memorandum on the SABHRS control environment to audit staff for consideration during their work. This audit addresses concerns regarding areas where SSB can improve controls over security access by not assigning users conflicting access roles, and limiting user access to modify SABHRS programming code and database tables.

Audit Objectives

This information systems audit focused on SABHRS operations and controls in place to ensure the application is accurately processing and storing financial and human resource (HR) records. Specifically, we addressed the following objectives:

1. Identify critical business processes for each module.
2. Provide assurances that modifications made to SABHRS have not altered critical SABHRS processes.
3. Identify application controls in place to ensure business processes are secure and working as expected.
4. Provide assurances over application controls identified through audit work.

Through audit work, we were able to determine critical processes are operating as intended. However, without strong security controls, SABHRS processes can be damaged or exploited. We conducted audit work addressing the audit objectives mentioned above, and that work is detailed in an internal memo provided to audit staff. The purpose of this report is to address security issues that can undermine SABHRS processing and

controls. Specifically, this report will cover excessive user access in the HR system and excessive access to programming code and database tables.

Audit Scope and Methodology

The scope of this audit included identification of SABHRS business processes and determining key controls in place to ensure SABHRS is processing as expected. Our audit work addressed processing within the Finance, Human Resource (HR), and Warrant Writer components of SABHRS.

Our work was performed by conducting interviews of SSB staff, query and analysis of SABHRS data, and observing SABHRS operations. In terms of general controls, we are relying on our recent audit of the DOA Data Center (#06DP-02), which houses SABHRS hardware and applications, to ensure general security controls. General controls include physical security, hardware maintenance, and user access.

The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office. We evaluated the control environment using state law and criteria established by ISACA's Control Objectives for Information and Technology.

Chapter II – SABHRS Incompatible Access Privileges

Introduction

In order for agency users to access the Statewide Accounting, Budgeting and Human Resource System (SABHRS), agency staff must be granted access to the application. SABHRS Services Bureau (SSB) has developed policy stating it is the responsibility of agency security officers to determine employees who need access and the level of access. SSB has created access roles to implement agency access decisions. These roles limit the screens in SABHRS a user can access and dictate if the user can view, change, or delete SABHRS information.

In many instances, a single user can be assigned multiple access roles. This is a concern as incompatible access roles can provide a user with privileges that can be used to exploit or damage the system. Based on our assessment of risk, we have identified user roles, that when assigned to a single user, present a considerable risk. Specifically, we identified agency users who have been assigned access roles allowing them to create a new employee record, and then enter and approve payroll time for that employee in SABHRS.

By assigning a single user access roles allowing these incompatible responsibilities, there is the potential SABHRS access could be used to create a fictitious employee, or add a fictitious employee to payroll. The Association of Certified Fraud Examiners (ACFE) has approximated 13 percent of all occupation fraud is the result of payroll fraud, like the creation of a fictitious employee. When a fictitious employee is added to payroll the employee who created the record will receive the payment. The ACFE estimates that an average of $55,000 is lost each time this fraud is committed.

Incompatible Access Roles in Human Resource Application

Through audit work, we identified 127 SABHRS HR users with access roles allowing them to create an employee record and then enter and approve time for that employee. SSB management represents these access roles are assigned by the agency security officers, and they do not consider limiting access to be their responsibility. Their position is that many smaller agencies do not have sufficient HR staff to segregate these duties among different users. However, of the 127 HR users we identified, a number of them work for larger agencies, such as the Department of Public Health and Human Services and the Department of Administration.

Because SSB management has not limited access, conflicting access roles have been assigned to agency users, increasing the potential for inappropriate activity. We

conducted further testing to determine if we could identify instances where conflicting access roles had a negative impact, such as the creation of a fictitious employee. Based on the data we had available to us, we did not identify any such instances.

Although SSB maintains they defer to agency security officers in assigning access, they are responsible for developing access roles and creating policy on how access to SABHRS is to be granted. As a result, they have the authority to develop access or system controls to prevent a single user from creating an employee, and then enter and approve time for the employee. Although SSB management believes limiting HR access could lead to an inconvenience in the administration of time and payroll, we consider the risk to the state to exceed agency need for this level of access.

RECOMMENDATION #1

We recommend the Department of Administration and the Statewide Accounting, Budgeting, and Human Resource System Services Bureau:

A. *Develop and implement procedures to identify conflicting access roles in the Statewide Accounting, Budgeting, and Human Resource System.*

B. *Develop and implement controls to ensure agency users cannot be assigned the conflicting access roles.*

SABHRS Change Controls Process

The production environment is where the operating version of a system is stored. Included in the production environment is programming code and database tables. Alteration of programming code and database tables can result in the disabling of critical functionality or the loss of sensitive data. To ensure this does not occur, industry standards suggest organizations implement change control procedures where modifications to a system are made in a test environment. Once the modification has been tested and monitored, and it has been determined the application is working as expected, the modification is migrated to the working version of the application in the production environment.

SSB has implemented a change control process to address modifications to SABHRS. For a modification to be made to the system, a written request is required from the user. Once the request has been reviewed by SSB, the modification will be developed and implemented into the test environment as industry standards suggest. However, we have identified SSB programers with access to modify SABHRS programming code and database tables directly in the production environment, bypassing the change control procedures they have implemented.

Excessive Access to Programming Code

There are currently ten SSB programmers with access to create, modify, and delete SABHRS programming code in the production environment. This access provides the ability to directly make changes to SABHRS functionality without testing for negative impact or appropriateness. Management represents access was granted when SABHRS was initially implemented to assist in the migration, but was not removed. They recognize the risk associated with allowing access to production programming code and have agreed to remove the access. We conducted additional audit work to ensure there have been no unauthorized changes to production code. Because SSB has not been monitoring changes to production programming code, we were unable to make a determination on unauthorized changes to programming code; however, we have determined SSB is working to remove this access.

Excessive Access to Database Tables

In addition to programmers with access to programming code, we also identified five SSB programmers with access to modify database tables in the production environment. By allowing this access, the potential for manipulated or lost data through erroneous or malicious activity increases. SSB states this access is required to trigger certain HR payroll processes and to troubleshoot and make application repairs in the Financial module. During a six-month period, we found 791 instances where programmers accessed SABHRS database tables. This includes two occasions where programmers accessed Accounts Payable (AP) voucher tables. Because programmers have access to modify voucher tables, the potential exists unauthorized or inadvertent changes could be made to voucher amounts paid to state vendors.

The AP module in SABHRS is used to create vouchers, resulting in payment to vendors. Application controls have been implemented to ensure the integrity of vouchers. Specifically, SABHRS requires an independent approval source when a voucher is created to verify the accuracy of vendor information and payment amount. Once vouchers have been entered and approved, the voucher records are stored in SABHRS database tables. SSB programmers who have constant access to modify voucher records, can change payment amounts and vendor information directly in the tables, thus bypassing the established change control procedures and the application controls designed to ensure voucher integrity.

Although SSB management states there is a need for programmers to access SABHRS database tables in production, we conclude the risk associated with excessive access to these tables exceeds the business need. Consequently, SSB should remove constant programmer access to the database tables and implement procedures to reinstate access during emergency situations.

RECOMMENDATION #2

We recommend the Department of Administration:

A. Remove programmer access allowing modification to programming code and database tables in the production environment.

B. Develop and implement procedures to provide temporary programmer access in emergency situations.

Department of Administration

Department Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

A-3

BRIAN SCHWEITZER, GOVERNOR — JANET R. KELLY, DIRECTOR

STATE OF MONTANA

(406) 444-2032
FAX (406) 444-6194

MITCHELL BUILDING
125 N. ROBERTS, RM 155
PO BOX 200101
HELENA, MONTANA 59620-0101

January 11, 2008

Mr. Scott Seacat, Legislative Auditor
Legislative Audit Division
State Capitol Building, Room 160
PO Box 201705
Helena MT 59620-1705

RE: Information Systems Audit #08DP03: Statewide Accounting, Budgeting and Human Resource System (SABHRS)

Dear Mr. Seacat:

The Department of Administration has reviewed the Information Systems Audit of the Statewide Accounting, Budgeting and Human Resource System (SABHRS) and the recommendations contained therein. Our response to the recommendations appears below:

Recommendation #1

We recommend the Department of Administration and the Statewide Accounting, Budgeting, and Human Resource System Services Bureau:

A. Develop and implement procedures to identify conflicting access roles in the Statewide Accounting, Budgeting, and Human Resource System.

B. Develop and implement controls to ensure agency users cannot be assigned the conflicting access roles.

Response

A. We concur. SABHRS has identified the conflicting Human Resource system access roles. SABHRS will implement procedures to audit the conflicting access roles to assure that appropriate access is granted.

B. We concur. SABHRS will develop and implement controls to prevent agency security officers from assigning conflicting roles. SABHRS will develop system edits to prevent these occurrences.

Recommendation #2

We recommend the Department of Administration:

A. Remove programmer access allowing modification to programming code and database tables in the production environment.

B. Develop and implement procedures to provide temporary programmer access in emergency situations.

Response

A. We concur. SABHRS will remove programmers' access to production database tables and programming code.

B. We concur. SABHRS will establish procedures to allow a programmer temporary access in an emergency situation. Emergency situations will be assessed on a case-by-case basis and authorized by the applicable system, process, and/or data owners. SABHRS will develop, document and implement procedures that provide complete audit trails when emergencies occur. SABHRS will identify, build and document application processes that allow other standard updates to production data to be performed by automated batch processes, process owners, or database administration staff.

My staff and I appreciated the courtesy and professionalism of the legislative audit staff in conducting this audit.

The Department's Corrective Action Plan (CAP) is enclosed.

Sincerely,

Janet R. Kelly, Director

Enclosure

Corrective Action Plan (CAP): Audit Report #08DP-03
Statewide Accounting, Budgeting, and Human Resource System
Department of Administration (DOA)
January 11, 2008

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management view	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**Recommendation #1** We recommend the Department of Administration (DOA) and the Statewide Accounting, Budgeting and Human Resource Systems Services Bureau (SABHRS): **A.** Develop and implement procedures to identify conflicting access roles in the Statewide Accounting, Budgeting, and Human Resource System. **B.** Develop and implement controls to ensure agency users cannot be assigned the conflicting access roles.	No		Concur	A. SABHRS has identified the conflicting Human Resource system access roles. SABHRS will implement procedures to audit the conflicting roles to assure that appropriate access is granted. B. SABHRS will develop and implement controls to prevent agency security officers from assigning conflicting access roles. SABHRS will develop system edits to prevent these occurrences.	Nyla Johnson Nyla Johnson	7/1/08 7/1/08
61010 DOA	**Recommendation #2** We recommend the Department of Administration: **A.** Remove programmer access allowing modification to programming code and database tables in the production environment. **B.** Develop and implement procedures to provide temporary programmer access in emergency situations.	No		Concur	A. SABHRS will remove programmers' access to production database tables and programming code. B. SABHRS will establish procedures to allow a programmer temporary access in an emergency situation. Emergency situations will be assessed on a case-by-case basis and authorized by the applicable system, process and/or data owners. SABHRS will develop, document	Nyla Johnson Nyla Johnson	5/1/08 5/1/08

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management view	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**Recommendation #2B continued**				and implement procedures that provide complete audit trails when emergencies occur. SABHRS will identify, build and document application processes that allow other standard updates to production data to be performed by automated batch processes, process owners, or database administration staff.		